SAVE
RETURN

COPY

Written June 1930
to June 30, 1927
& passed from
the Bureau of Foreign
Control (Justice
Department) to the
Bureau of Customs
in July 1931 the
Cryptanalytical
Unit moved up
to the
Coast Guard
Traffic Section
where interception
was

HISTORY OF WORK IN CRYPTANALYSIS

APRIL 1921 -- JUNE 1930
1927

******

The cryptanalyst of the Treasury Department reports the following work covered between April 1927, and June, 1930:

In the spring of 1927, there had accumulated in the Coast Guard Intelligence Office an enormous number of messages in secret correspondence. This traffic covered a period of more than a year, was from many different sources both on the Atlantic and Pacific Coasts, and the volume was increasing daily. Upon the first date above, work of solution was begun upon the hundreds of messages on file. Within two months the great mass of accumulated traffic was reduced from unknown to known. Then, since the sources of secret traffic were increasing, different divisions of the Treasury Department, notably Foreign Control and Coast Guard, cooperated in plans to launch an intelligence service based upon the reading of secret illegal correspondence, which might fall into its hands.

PACIFIC COAST

The Coast Guard base at San Pedro, California, forwarded to Headquarters in May and June of 1927, a series of messages which were the means of breaking into the systems in current use on the Pacific Coast. At that time two fleets of rum vessels were working on the Pacific Coast, operated by rival Canadian firms, one generally characterized as the Hobbs interests, the other known as the Consolidated Exporters Corporation, both of Vancouver.

About this time I began to receive messages from San Francisco which dealt with activities along the Pacific Coast from Vancouver to Ensenada. As rapidly as the systems were broken, each day's traffic was translated by me into plain

COPY

Written June 1931

HISTORY OF WORK IN CRYPTANALYSIS

APRIL 1927 -- JUNE 1930

******

The cryptanalyst of the Treasury Department reports the following work covered between April 1927, and June, 1931:

In the spring of 1927, there had accumulated in the Coast Guard Intelligence Office an enormous number of messages in secret correspondence. This traffic covered a period of more than a year, was from many different sources both on the Atlantic and Pacific Coasts, and the volume was increasing daily. Upon the first date above, work of solution was begun upon the hundreds of messages on file. Within two months the great mass of accumulated traffic was reduced from unknown to known. Then, since the sources of secret traffic were increasing, different divisions of the Treasury Department, notably Foreign Control and Coast Guard, cooperated in plans to launch an intelligence service based upon the reading of secret illegal correspondence, which might fall into its hands.

PACIFIC COAST

The Coast Guard base at San Pedro, California, forwarded to Headquarters in May and June of 1927, a series of messages which were the means of breaking into the systems in current use on the Pacific Coast. At that time two fleets of rum vessels were working on the Pacific Coast, operated by rival Canadian firms, one generally characterized as the Hobbs interests, the other known as the Consolidated Exporters Corporation, both of Vancouver.

About this time I began to receive messages from San Francisco which dealt with activities along the Pacific Coast from Vancouver to Ensenada. As rapidly as the systems were broken, each day's traffic was translated by me into plain

text. When the material revealed was such as could be of immediate use, it was telegraphed in cipher to the Pacific Coast. If not of immediate importance it was forwarded by air mail.

This plan of solving all traffic in Washington and forwarding the plain text to the Pacific Coast was continued until May 1928, when the enforcement agencies on the West Coast strongly urged that the Cryptanalyst proceed to San Francisco for the purpose of instructing some person there how to transcribe the messages from code and cipher into plain text, in order to make information therein immediately available.

This request was complied with, and in June and July, 1928, I preceeded to California and stopped first at San Pedro where I obtained from the Coast Guard a mass of information extremely useful in solving the secret systems in use; and from there I proceeded to San Francisco, where it was agreed that Mr. C.A. Housel, of the office of the Coordinator of the Pacific Coast Details, should be instructed in methods of transcribing the traffic from code and cipher into plain language. Mr. Housel proved to be of a very industrious andpainstaking disposition and soon showed capability for the work of transcription. Both Mr. Housel and Mr. Clarence E Reeves, radio operator, were of the greatest assistance in identifying the various vessels operating, and in furnishing subsidiary information useful to me in the breaking down of new systems.

From July 1928, to the present time this procedure has been followed in reference to Pacific Coast messages. All traffic forwarded to Washington is classified and indexed, and as soon as a new system is solved, the explanation, vocabulary and modus operandi for it are forwarded to Mr. Housel who then is enabled to convert into plain text the messages immediately upon receiving them.

In a report from Mr. Housel to the Commissioner of Prohibition under date of January 29, 1930, he states that the messages passing between Vancouver

and vessels operating on the Pacific Coast between May, 1928, and January, 1930, number 3300. This number comprises correspondence passing between four or five shore stations and approximately 25 vessels. Nearly fifty distinct and separate systems of secret communication have been employed, and in many cases what is termed one system, that is, the means used to read the messages, comprises the use of from three to five methods within the one system, each of which must be solved as an entity in itself. At no time during the World War, when secret methods of communication reached their highest development, were there used such involved ramifications as are to be found in some of the correspondence of West Coast rum running vessels.

During the past two years, the systems have increased constantly in complexity and in number; whereas in 1927-1928 only two general systems were in use, these changing approximately every six months; at the present time there is a different system for practically every boat and vessel operating on the Pacific Coast. Some of these are of a complexity never even attempted by any government for its most secret communications. No one of the systems could be characterized as simple. The accompanying chart presents generally the Pacific Coast Correspondence in May 1930. In all cases, as heretofore stated, a new system is solved in this office as soon as sufficient traffic and the degree of complexity will permit, and the method is then disclosed to Mr. Housel, who reads the messages daily as they are reported to him. Although to date Mr. Housel's aptitude for this work has not reached the point of solving a new system, his powers of inference and his sources of information have been of great benefit and usefulness in the pursuance of the work at headquarters.

THE GULF COAST

During the development of smuggling on the Pacific Coast within the last year and the merging of most of the interests there into the Consolidated

Exporters Corporation, there has also been evident extended operations into other waters by this large company with headquarters at Vancouver. Consolidated Corporation agents have been sent not only to Mexico and Belize, but to Havana, New Orleans, Miami, Nassau, and Montreal. Thus a network of activities by this one company alone, completely surrounds the United States. Large operations, with headquarters at Belize, began in the autumn of 1929 with one vessel and have since increased to four, possibly five. All agents and operations are in direct communication with Vancouver headquarters.

Secret messages relating to smuggling on the Gulf Coast at present number several hundred a month. This traffic is of a diverse nature, differing with almost every few messages. It concerns innumerable agents, vast amounts of money, and extensive activities.

In October and November of 1929, at the request of the Customs Service, I spent a month in Houston, Texas, solving a mass of traffic which had been suppoenaed by the United States Attorney and which related to smuggling on the Gulf Coast. The material turned over to Customs officers as a result, numbered approximately 650 messages, employing 24 different systems of secret correspondence. Since then the number of messages and types of correspondence in solved traffic have increased constantly, and these have been regularly forwarded to the Customs Service

THE ATLANTIC COAST

The Florida coast has been a prolific source of secret messages. For three years the daily volume has been on the whole increased, the number of messages reaching my desk at the present time amounting to about 25 daily. The correspondence usually passes between various points in Florida and Georgia on the one hand, and Havana and Nassau on the other.

The other main sources of smuggling traffic on the Atlantic Coast is,

of course, the region around New York. In a single report of a radio inspector of the Department of Commerce in February 1920, the report covering five days only of activities in ascertaining unlicensed radio stations, it is stated that within that time no less than 45 unlicensed stations were heard, all within a 10-mile radius of New York City. The traffic forwarded to my desk by him was all in codes and ciphers and all stations were engaged in rum running operations . In addition, traffic in secret correspondence has come in from every Coast Guard Patrol area on the Atlantic Coast.

The solved messages show operations extending from Nova Scotia to Bermuda, the Bahamas and Havana, and touching all points of the United States along the coast which are favorable for smuggling.

MISCELLANEOUS

In addition to the enormous volume of secret messages solved during the past three years which pertained to the international phase of liquor smuggling, there has also been a considerable volume pertaining to the smuggling of narcotics and aliens. Some messages also have been solved for the Bureau of Internal Revenue pertaining to evasions of the Income Tax Laws. I have also been summoned in court cases to testify as an expert witness upon secret messages.

SUMMARY

The past three years are thus shown to cover a range of work done for the Bureau of Customs, the Coast Guard, the Bureau of Narcotics, the Bureau of Internal Revenue, the Prohibition Bureau, and the Department of Justice. Secret traffic has been solved amounting to 12,000 messages, which covered activities touching upon the Pacific Coast from Vancouver to Ensenada; from Belize along the Gulf Coast to Tampa; from Key West to Savannah, including Havana and the Bahamas; and from New Jersey to Maine, operations including the Bermudas, St. Pierre and Newfoundland. The above number comprises only messages which were pertinent to the services

requesting their solution. It does not include the total number of messages examined and discarded. This total amounts to approximately 25,000 messages annually.

CONCLUSION

It is perhaps difficult for anyone who has never attempted to read secret correspondence, to understand just what are the processes involved. Of the two great classes of secret methods of correspondence, that is code and cipher, either or both may be employed within one message. The most elementary of the cipher systems may be broken with only a small amount of text, frequently with a single message. This method, however, is now very little used.

Code systems require a larger amount of text for solution, comprising as they do, conventionalized dictionaries wherein a single code group such as AVAST or QUJER may mean a whole phrase or even a whole sentence. There are many public and commercial codes on the market, and a common device used by smugglers is to apply some system of cipher to some such code book. From a cryptanalyst's standpoint, a process of experimentation is necessary to ascertain the cipher which has been added to the code. Sometimes a numeral termed an additive is employed. In other cases substitutions of letters may be made for the letters of the original code group; or again, a combination of all these methods may be employed, even to the extent of using more than one code book. One such system solved in early 1928 passed through the following steps:

The correspondent prepared a message for sending by finding the plain language in the ABC code, 6th Edition, and the numberal code group therein was recorded. To this number was added 1000. The resulting number was then found not in the same code book but in the Acme Code. Here the letter group opposite the number was recorded and then to this was applied a mixed cipher alphabet. The resulting letters were then sent out as the secret message. This process, which takes so little time to describe, is in reality very laborious, and taken an infinitely

longer time to transcribe, even by the correspondents thoroughly familiar with the modus operandi .

Now to the non-expert all secret messages present the same appearance. But to the experienced eye a casual inspection will reveal many facts. In this case an inspection determined that the system employed came under the general classification of Enciphered Code. Then began what seemed endless experimentation to determine the particular type of enciphered code. There are hundreds of public codes any one of which might have been used, and in order to discover which, it was necessary to solve the cipher applied. With enormous difficulty the cipher alphabet was built up, by which the groups actually appearing in the message were resolved into code groups of the Acme Code. But as this resulted in no intelligible meaning, it was obvious that further steps were necessary in order to reach clear language. The processes of experiment continued, the search among hundreds of code books was again prosecuted, and finally the whole laborious process was revealed.

An actual message in this system will illustrate the methods involved:

Message as sent:	MJFAK	ZYWKH	QATTT	JSL	QATS	QSYGX	OGFB
Cipher alphabet applied resulting			where	and	when		fuel
in Acme letters:	BARHY	OIJYS				WINUM	
Acme code numbers	08033	53725				25536	
Subtract 1000	07033	52725				24536	
ABC code, 6th Edition	Anchored	in harbor	"	"	"	are you sending	"

Message: Anchored in harbor. Where and when are you sending fuel?

Many times, in fact most frequently, the plain text meanings are not to be found in any known code. The code groups themselves may be taken from a commonly used book but the meanings are arbitrarily supplied by the users. In such a case the vocabulary must be built up, or in other words, their code book must be reconstructed. This frequently must be done in addition to discovering

whatever method or methods of encipherment may have been used in connection with the code. This may be a constantly changing system such as utilizing the day of the week or month; or it may be a complex system of spelling or of numeral additives of any number up to 2000.

Any report limited in scope, such as this, can only hint at the varieties and types of secret correspondence which are encountered. These varieties have a wide range and their degree of complexity differ as primary arithmetic differs from analytical geometry and include all intervening stages. The primary or elementary types are by far the most uncommon today. Furthermore, it is not only the problem of the expert to solve systems when classified, but even after systems are classified, it is many times a matter of considerable difficulty to determine into which of several known systems a given message will fall. For example, in the accompanying chart, systems A to I yield messages of such similar appearance that an extremely specialized technique is required to place the messages in the proper classification. Long experience and the keenest sort of analysis is necessary in order to classify such traffic alone, without the attendant work of solution.

ELIZABETH SMITH FRIEDMAN
Cryptanalyst

This message was written at the time I was on the payroll of the Bureau of Customs, Coast Guard Headquarters

In July 1931, the cryptanalytic Section at Coast Guard Headquarters was created with me as Chief, on payroll of C.G. Hq. & T.